

A LOCAL-GLOBAL PRINCIPLE FOR POWER MAPS

N. JONES

ABSTRACT. Let f be a function from the set of rational numbers into itself. We call f a global power map if $f(\alpha) = \alpha^k$ for some integer exponent k . We call f a local power map at the prime number p if f induces a well-defined group homomorphism on the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$. We conjecture that if f is a local power map at an infinite number of primes p , then f must be a global power map. Our main theorem implies that if f is a local power map at every prime p in a set with positive upper density relative to the set of all primes, then f must be a global power map. In particular, this represents progress towards a conjecture of Fabrykowski and Subbarao.

1. INTRODUCTION

Let $\mathbb{N} := \{1, 2, 3, \dots\}$ denote the set of natural numbers and for any prime number p , define

$$\mathbb{N}_{(p)} := \{n \in \mathbb{N}; p \nmid n\}.$$

Given a function

$$f : \mathbb{N} \longrightarrow \mathbb{N},$$

suppose that p is a prime for which

$$f(\mathbb{N}_{(p)}) \subseteq \mathbb{N}_{(p)}.$$

For such a prime p , one may ask whether there exists a multiplicative group homomorphism $f_p : \mathbb{F}_p^\times \longrightarrow \mathbb{F}_p^\times$ for which the diagram

$$\begin{array}{ccc} \mathbb{N}_{(p)} & \xrightarrow{f} & \mathbb{N}_{(p)} \\ \text{red}_p \downarrow & & \text{red}_p \downarrow \\ \mathbb{F}_p^\times & \xrightarrow{f_p} & \mathbb{F}_p^\times \end{array} \quad (1)$$

commutes. We consider the set S_f of such primes:

$$S_f := \{p \text{ prime}; f(\mathbb{N}_{(p)}) \subseteq \mathbb{N}_{(p)} \text{ and } \exists \text{ a homomorphism } f_p \text{ for which (1) commutes}\}.$$

For instance, if $f(n) = n^2$ for all $n \in \mathbb{N}$, then one has $S_f = \{\text{all primes}\}$. On the other hand, suppose f is defined by

$$f(n) = \begin{cases} 7 & \text{if } n \equiv 0 \pmod{3} \\ 3\pi(n) + 1 & \text{if } n \equiv 1 \pmod{3} \\ 3\nu(n) + 2 & \text{if } n \equiv 2 \pmod{3}, \end{cases}$$

where (here and throughout the paper) $\pi(n) := |\{\text{primes } p : p \leq n\}|$ and $\nu(n) := |\{\text{primes } p : p \text{ divides } n\}|$. Then $3 \in S_f$, and quite probably $S_f = \{3\}$. By using a diagonalization argument, one can construct functions f which certainly satisfy $S_f = \{3\}$. By incorporating the Chinese Remainder Theorem, given any *finite* set of primes S one can find a function f for which $S_f = S$. Our motivating question is the following.

Question 1.1. *Does there exist a function $f : \mathbb{N} \longrightarrow \mathbb{N}$ for which S_f is infinite and $S_f \neq \{\text{all primes}\}$?*

This work was partially supported by a Ralph E. Powe Junior Faculty Enhancement award and also by NSA grant H98230-12-1-0210. The author gratefully acknowledges Oak Ridge Associated Universities and the National Security Agency for this support.

We will presently couch this question in slightly different terms. Returning to (1), note that since \mathbb{F}_p^\times is cyclic, any multiplicative homomorphism $f_p : \mathbb{F}_p^\times \rightarrow \mathbb{F}_p^\times$ must be of the form $f_p(x) = x^{k_p}$ for some exponent $k_p \in \mathbb{Z}/(p-1)\mathbb{Z}$. In particular,

$$S_f = \{p \text{ prime}; \exists k_p \in \mathbb{Z}/(p-1)\mathbb{Z} \text{ for which } \forall n \in \mathbb{N}_{(p)}, \quad f(n) \equiv n^{k_p} \pmod{p}\}.$$

Definition 1.2. Let S be a set of prime numbers. A function $f : \mathbb{N} \rightarrow \mathbb{N}$ is a **local power map at S** if $S \subseteq S_f$.

Definition 1.3. A function $f : \mathbb{N} \rightarrow \mathbb{N}$ is called a **global power map** if there is an exponent $k \in \mathbb{N} \cup \{0\}$ such that, for each $n \in \mathbb{N}$ one has $f(n) = n^k$.

Note that any global power map f is a local power map at $S = \{\text{all primes}\}$, and so in particular is a local power map at an infinite set of primes. The main result of [7] (or even of its predecessor [6]), implies that there exists a prime number q for which the set

$$\{p \text{ prime}, \langle q \pmod{p} \rangle = \mathbb{F}_p^\times\}$$

is infinite. Using this fact, one may deduce that any local power map at $S = \{\text{all primes}\}$ must be a global power map. Thus, Question 1.1 may be stated equivalently as

Question 1.4. *Does there exist a function $f : \mathbb{N} \rightarrow \mathbb{N}$ which is a local power map at an infinite set of primes, but which is not a global power map?*

We will provide heuristics which lead us to conjecture that the answer is no:

Conjecture 1.5. *Suppose $f : \mathbb{N} \rightarrow \mathbb{N}$ is a local power map at an infinite set of primes (i.e. suppose that $|S_f| = \infty$). Then f must be a global power map.*

The preceding discussion applies just as well when we replace \mathbb{N} with the set \mathbb{Q} of rational numbers. Indeed, for any prime number p let us employ the standard notation

$$\begin{aligned} \mathbb{Z}_{(p)} &:= \left\{ \frac{n}{m} \in \mathbb{Q} : p \nmid m \right\}, \\ \mathbb{Z}_{(p)}^\times &= \left\{ \frac{n}{m} \in \mathbb{Z}_{(p)} : p \nmid n \right\}, \end{aligned}$$

where the fraction n/m above is assumed to be in lowest terms. As is well-known, $\mathbb{Z}_{(p)}$ is a local ring with maximal ideal $p\mathbb{Z}_{(p)}$, and one has an isomorphism

$$\frac{\mathbb{Z}_{(p)}}{p\mathbb{Z}_{(p)}} \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}.$$

For $\alpha, \beta \in \mathbb{Z}_{(p)}$, we write $\alpha \equiv \beta \pmod{p}$ provided $\alpha - \beta \in p\mathbb{Z}_{(p)}$. Now if

$$f : \mathbb{Q} \rightarrow \mathbb{Q}$$

is any function, we consider the set

$$S_f := \{p \text{ prime}; \exists k_p \in \mathbb{Z}/(p-1)\mathbb{Z} \text{ such that } \forall \alpha \in \mathbb{Z}_{(p)}^\times, \quad f(\alpha) \equiv \alpha^{k_p} \pmod{p}\}.$$

Definition 1.6. Let S be a set of prime numbers. A function $f : \mathbb{Q} \rightarrow \mathbb{Q}$ is a **local power map at S** if $S \subseteq S_f$, and f is a **global power map** if, for some integer $k \in \mathbb{Z}$, one has

$$\forall \alpha \in \mathbb{Q}, \quad f(\alpha) = \alpha^k.$$

We make the following conjecture, which (as we will show in Section 3) implies Conjecture 1.5.

Conjecture 1.7. *Suppose that $f : \mathbb{Q} \rightarrow \mathbb{Q}$ is a local power map at an infinite set of primes (i.e. suppose that $|S_f| = \infty$). Then f must be a global power map.*

Remark 1.8. Conjecture 1.7 also implies Conjecture 3.1 of [3], which states that any quasi-multiplicative function $f : \mathbb{N} \rightarrow \mathbb{Z}$ which is not identically zero and satisfies

$$f(n+p) \equiv f(n) \pmod{p}$$

for infinitely many primes p must be a global power map. This connection will be discussed in more detail in Section 3.

In the present paper, we will prove the following weakened version of Conjecture 1.7, in which “ S_f is infinite” is replaced by “ S_f has positive upper density in the primes.” For any set S of prime numbers, define

$$S(x) := \{p \in S : p \leq x\}$$

and the upper density

$$\bar{\delta}(S) := \limsup_{x \rightarrow \infty} \frac{|S(x)|}{\pi(x)}.$$

We will prove the following theorem.

Theorem 1.9. *Let $f : \mathbb{Q} \rightarrow \mathbb{Q}$ be any function which is not a global power map. Then there exist real constants $b_f, c_f > 0$ so that for $x \geq c_f$, the bound*

$$|S_f(x)| \ll \frac{\log \log \log \log x}{\log \log \log x} \cdot \pi(x) + b_f$$

holds, with an absolute implied constant. In particular, if $f : \mathbb{Q} \rightarrow \mathbb{Q}$ is a function for which $\bar{\delta}(S_f) > 0$, then f is a global power map.

Our proof of this theorem applies an effective version of the Chebotarev density theorem of Lagarias and Odlyzko to certain Kummer extensions attached to the function f .

2. NOTATION

Throughout the paper, we will use the following notation. For $\alpha \in \mathbb{Q}$ and a prime number p , there is a unique integer c for which $\alpha = p^c \cdot (a/b)$, where $a, b \in \mathbb{Z}$ and $p \nmid ab$. We then define $\text{ord}_p(\alpha) := c$. Furthermore, we define $\text{Num}(\alpha) := n$ and $\text{Den}(\alpha) := m$ where $\alpha = n/m \in \mathbb{Q}$ is written in lowest terms. We use the symbols $O(\cdot)$ and \ll in the usual ways, namely if $f, g : [\gamma, \infty) \rightarrow \mathbb{C}$ are complex functions then we write

$$f = O(g), \quad \text{or equivalently} \quad f \ll g$$

if there is a positive constant C for which $|f(x)| \leq C|g(x)|$ for all $x \in [\gamma, \infty)$. In case there is an auxiliary parameter y upon which the implied constant C depends, we will indicate this with a subscript, so that

$$f = O_y(g) \quad \text{or equivalently} \quad f \ll_y g$$

is used to indicate that $|f(x)| \leq C(y)|g(x)|$, where the $C(y)$ may depend on y but not on x . We write $f(x) \sim g(x)$ as $x \rightarrow \infty$ to mean that $f(x)$ is asymptotic to $g(x)$ as $x \rightarrow \infty$, i.e. to mean that $\lim_{x \rightarrow \infty} f(x)/g(x) = 1$. When used as variables, the letters p and ℓ will always denote prime numbers. We will occasionally denote the reduction modulo p map by

$$\begin{aligned} \mathbb{Z}_{(p)} &\rightarrow \mathbb{F}_p \\ n &\mapsto \hat{n}. \end{aligned}$$

For an odd prime number ℓ , let ζ_ℓ denote a primitive ℓ -th root of unity. In our discussion of Kummer extensions, we will employ the following vector notation. For $m \geq 0$ and $\mathbf{c} = (c_1, c_2, \dots, c_m) \in (\mathbb{Q}^\times)^m$, we define

$$\mathbb{Q}(\zeta_\ell, \mathbf{c}^{1/\ell}) := \mathbb{Q}(\zeta_\ell, c_1^{1/\ell}, c_2^{1/\ell}, \dots, c_m^{1/\ell}),$$

where if $m = 0$ we make the interpretation $\mathbb{Q}(\zeta_\ell, \mathbf{c}^{1/\ell}) := \mathbb{Q}(\zeta_\ell)$. Furthermore, for a vector $\mathbf{n} = (n_1, n_2, \dots, n_m) \in \mathbb{Z}^m$, we will use the notation

$$\mathbf{c}^{\mathbf{n}} := \prod_{i=1}^m c_i^{n_i} \in \mathbb{Q}^\times.$$

3. RELATED RESULTS

We now give a brief survey of various related results (each with slightly different hypotheses on the integer-valued function f , but with the conclusion “then f is a global power map,” or a closely related conclusion). Before doing so, let us make a few elementary observations and show why Conjecture 1.7 implies Conjecture 1.5.

Lemma 3.1. *Suppose that $f : \mathbb{Q} \rightarrow \mathbb{Q}$ is a function for which S_f is infinite. Then*

$$f(\mathbb{Q}^\times) \subseteq \mathbb{Q}^\times, \quad (2)$$

and the restriction of f to \mathbb{Q}^\times is completely multiplicative, i.e. for any $\alpha, \beta \in \mathbb{Q}^\times$ one has

$$f(\alpha\beta) = f(\alpha)f(\beta). \quad (3)$$

Proof. To prove (2), fix $\alpha \in \mathbb{Q}^\times$. If $f(\alpha) = 0$ then for each prime p ,

$$\text{ord}_p(\alpha) = 0 \implies p \notin S_f, \quad (4)$$

implying that S_f is finite, a contradiction. Thus, (2) holds. The second assertion (3) follows from the observation that, for any $\gamma \in \mathbb{Q}$,

$$\gamma \equiv 0 \pmod{p} \text{ for infinitely many primes } p \implies \gamma = 0, \quad (5)$$

which is true since if $\gamma = a/b$ in lowest terms then $\gamma \equiv 0 \pmod{p}$ if and only if p divides a .

To prove that f is completely multiplicative, fix $\alpha, \beta \in \mathbb{Q}^\times$ and apply (5) to $\gamma = f(\alpha\beta) - f(\alpha)f(\beta)$, which is divisible by every prime $p \in S_f$ for which $\text{ord}_p(\alpha) = \text{ord}_p(\beta) = 0$. Since S_f is infinite, there are infinitely many such primes p . This concludes the proof. \square

In particular, if $f : \mathbb{Q} \rightarrow \mathbb{Q}$ and S_f is infinite, then $f|_{\mathbb{Q}^\times}$ is uniquely determined by its values on $\{-1\} \cup \{\text{all primes}\}$. We will now show why Conjecture 1.7 implies Conjecture 1.5, which amounts to proving the following lemma. Since we will be varying a bit the domain of the function f , let us first write down the general situation, which encapsulates the set-up in both of the conjectures given in the introduction.

If $A \subseteq \mathbb{Q}$ is a subset which is closed under multiplication, then the set

$$A_{(p)} := A \cap \mathbb{Z}_{(p)}^\times$$

is also closed under multiplication. Furthermore, if

$$f : A \rightarrow \mathbb{Q}$$

is any function, then we may define the set S_f of primes as before by

$$S_f := \{p \text{ prime}; \exists k_p \in \mathbb{Z}/(p-1)\mathbb{Z} \text{ such that } \forall \alpha \in A_{(p)}, \quad f(\alpha) \equiv \alpha^{k_p} \pmod{p}\}.$$

Lemma 3.2. *Suppose that $f : \mathbb{N} \rightarrow \mathbb{Q}$ is any function for which S_f is infinite. Then there is a completely multiplicative function*

$$\tilde{f} : \mathbb{Q} \rightarrow \mathbb{Q}$$

such that $\forall n \in \mathbb{N}$, $\tilde{f}(n) = f(n)$ and for which $S_{\tilde{f}}$ is infinite.

Proof. First of all, by the same reasoning as in (4), the infinitude of S_f implies that

$$\forall n \in \mathbb{N}, \quad f(n) \neq 0. \quad (6)$$

Furthermore, by the same reasoning as in the proof of (3) one sees that f is completely multiplicative. In particular,

$$f(1) = 1.$$

We begin by extending f to a function $f_1 : \mathbb{Z} \rightarrow \mathbb{Q}$. Note that for odd $p \in S_f$, since $k_p \in \mathbb{Z}/(p-1)\mathbb{Z}$, the parity of k_p is well-defined, and by the pigeon-hole principle, either k_p is infinitely often even or it is infinitely often odd. We set

$$\nu_f := \begin{cases} 0 & \text{if } k_p \text{ is even for infinitely many } p \in S_f \\ 1 & \text{otherwise,} \end{cases}$$

and then define $f_1 : \{-1, 0, 1\} \longrightarrow \{-1, 0, 1\}$ by

$$f_1(\pm 1) := (\pm 1)^{\nu_f} \quad \text{and} \quad f_1(0) := 0.$$

Then, for each $x, y \in \{-1, 0, 1\}$ one has $f_1(xy) = f_1(x)f_1(y)$. Furthermore, if $\text{sgn} : \mathbb{Z} \longrightarrow \{-1, 0, 1\}$ is defined by

$$\text{sgn}(n) := \begin{cases} \frac{n}{|n|} & \text{if } n \neq 0 \\ 0 & \text{if } n = 0, \end{cases}$$

then any $n \in \mathbb{Z}$ decomposes as $n = \text{sgn}(n) \cdot |n|$, and we define

$$f_1(n) := f_1(\text{sgn}(n)) \cdot f(|n|).$$

It follows that $f_1 : \mathbb{Z} \longrightarrow \mathbb{Q}$ is completely multiplicative and (by (6)) satisfies

$$n \neq 0 \implies f_1(n) \neq 0. \tag{7}$$

Furthermore,

$$S_{f_1} \supseteq \{p \in S_f : (-1)^{k_p} = (-1)^{\nu_f}\},$$

and by construction the right-hand set is infinite. We now extend f_1 to all of \mathbb{Q} by setting

$$\tilde{f}\left(\frac{n}{m}\right) := \frac{f_1(n)}{f_1(m)}.$$

Since f_1 is completely multiplicative (and by (7)), \tilde{f} is well-defined, is completely multiplicative, and satisfies $S_{f_1} \subseteq S_{\tilde{f}}$. This proves the lemma. \square

By the Lemma 3.1, one may as well add “ f is completely multiplicative” to the hypothesis of Conjecture 1.7. More generally, recall that f is called *multiplicative* if $f(nm) = f(n)f(m)$ whenever $\gcd(m, n) = 1$.

It follows from a result of P. Erdős [2, Theorem V] that

$$\left(\begin{array}{l} f : \mathbb{N} \longrightarrow \mathbb{N} \text{ is multiplicative} \\ \text{and } \forall n \in \mathbb{N}, f(n+1) \geq f(n) \end{array} \right) \implies f \text{ is a global power map.}$$

Replacing the monotonicity hypothesis with the condition

$$\forall n \in \mathbb{N}, \quad f(n+k) \equiv f(n) \pmod{k}, \tag{8}$$

M. V. Subbarao [13] has shown that

$$\left(\begin{array}{l} f : \mathbb{N} \longrightarrow \mathbb{Z} \text{ is multiplicative} \\ \text{and satisfies (8) for all } k \in \mathbb{N} \end{array} \right) \implies \left(\begin{array}{l} f \text{ is a global power map} \\ \text{or } f(n) = 0 \quad \forall n \in \mathbb{N}. \end{array} \right)$$

In [3] Subbarao and J. Fabrykowski prove a similar theorem, with the multiplicativity of f relaxed a bit (as we presently describe), and where (8) is only demanded for *primes* k , i.e.

$$\forall n \in \mathbb{N}, \quad f(n+p) \equiv f(n) \pmod{p}. \tag{9}$$

The following is equivalent to [3, Definition 1.3]

Definition 3.3. A function $f : \mathbb{N} \longrightarrow \mathbb{N}$ is called *quasi-multiplicative* if, for any $n \in \mathbb{N}$ and any prime p not dividing n , one has

$$f(pn) = f(p)f(n).$$

For any function $f : \mathbb{N} \longrightarrow \mathbb{Z}$, let us define the set

$$T_f := \{p \text{ prime; (9) holds}\}. \tag{10}$$

In [3] it is shown that

$$\left(\begin{array}{l} f : \mathbb{N} \longrightarrow \mathbb{Z} \text{ is quasi-multiplicative} \\ \text{and } T_f = \{\text{all primes}\} \end{array} \right) \implies \left(\begin{array}{l} f \text{ is a global power map} \\ \text{or } f(n) = 0 \quad \forall n \in \mathbb{N}. \end{array} \right)$$

Furthermore, they make the following conjecture.

Conjecture 3.4. *If $f : \mathbb{N} \longrightarrow \mathbb{Z}$ is quasi-multiplicative and T_f is infinite, then either $f(n) = 0$ for each $n \in \mathbb{N}$ or f is a global power map.*

The next lemma, taken together with Lemma 3.2, shows that Conjecture 3.4 is implied by Conjecture 1.7. Note that, for any $p \in T_f$, there is a well-defined function

$$f_p : \mathbb{F}_p \longrightarrow \mathbb{F}_p, \quad f_p(n \pmod{p}) := f(n).$$

Lemma 3.5. *Suppose that $f : \mathbb{N} \longrightarrow \mathbb{Z}$ is quasi-multiplicative and that T_f is infinite. Then either $f(n) = 0$ for each $n \in \mathbb{N}$, or $T_f - (S_f \cap T_f)$ is finite (and thus S_f is infinite).*

Proof. Fix any prime $p \in T_f$ and note that $p \in S_f \cap T_f$ if and only if

$$f_p(\mathbb{F}_p^\times) \subseteq \mathbb{F}_p^\times \tag{11}$$

holds and f_p is a multiplicative homomorphism. Let

$$\begin{aligned} \mathbb{Z} &\rightarrow \mathbb{F}_p \\ n &\mapsto \hat{n} \end{aligned}$$

denote the reduction modulo p map and choose $g \in \mathbb{N}$ so that $\langle \hat{g} \rangle = \mathbb{F}_p^\times$. Suppose that (11) does not hold, i.e. that $f_p(\hat{g}^n) = \hat{0}$ for some positive integer n . By Dirichlet's theorem on primes in arithmetic progressions, one may find n prime numbers q_1, q_2, \dots, q_n for which

$$\forall i \in \{1, 2, \dots, n\}, \quad q_i \equiv g \pmod{p}.$$

It follows from Definition 3.3 that

$$\hat{0} = f_p(\hat{g}^n) = f_p\left(\prod_{i=1}^n \hat{q}_i\right) = \prod_{i=1}^n f_p(\hat{q}_i) = (f_p(\hat{g}))^n, \tag{12}$$

and so we conclude that, for any prime $p \in T_f$,

$$\text{condition (11) fails} \implies f_p(\mathbb{F}_p) = \{\hat{0}\}.$$

Furthermore, if we set

$$T_0 := \{p \in T_f : f_p(\mathbb{F}_p) = \{\hat{0}\}\},$$

then for each $n \in \mathbb{N}$, $f(n)$ is divisible by every prime $p \in T_0$. Thus,

$$|T_0| = \infty \implies \forall n \in \mathbb{N}, f(n) = 0.$$

Assuming f is not identically zero, we have that T_0 is finite, and putting $S := T_f - T_0$, we see that (11) holds for each $p \in S$. Furthermore, using Dirichlet's theorem on primes in arithmetic progressions and reasoning as in (12), one sees that the restriction of f_p to \mathbb{F}_p^\times is a multiplicative homomorphism for each $p \in S$. In particular, $S = T_f \cap S_f$, which concludes the proof. \square

Remark 3.6. Lemmas 3.5 and 3.1 together imply that any quasi-multiplicative function satisfying (9) for infinitely many primes p is necessarily completely multiplicative, solving Problem 3.9 of [3].

The main result of [4] implies that, if the set $\{\text{all primes}\} - T_f$ is finite, then either f is identically zero or f is a global power map. A somewhat stronger result may be found in [8, Proposition 1, p. 329] (whose proof appeals to [1, Theorem 1]), which implies that if T_f has density one in the set of primes, then either f is identically zero or f is a global power map. Putting Lemmas 3.5 and 3.2 together with Theorem 1.9, we obtain the following corollary, which represents further progress towards Conjecture 3.4.

Corollary 3.7. *Let $f : \mathbb{N} \longrightarrow \mathbb{Z}$ be a quasi-multiplicative function and let T_f be defined by (10). Then either f is identically zero, or f is a global power map, or there exist real constants $b_f, c_f > 0$ so that, for $x \geq c_f$, the bound*

$$|T_f(x)| \ll \frac{\log \log \log \log x}{\log \log \log x} \cdot \pi(x) + b_f$$

holds, with an absolute implied constant. In particular, if $f : \mathbb{N} \longrightarrow \mathbb{Z}$ is a quasi-multiplicative function for which $\bar{\delta}(T_f) > 0$, then either f is identically zero or f is a global power map.

Returning to our survey of related results, one may also replace the assumption of (quasi-)multiplicativity of f by upper bounds on its growth. In this spirit, I. Ruzsa [11] proved that, if $f : \mathbb{N} \rightarrow \mathbb{Z}$ satisfies (8) for each $k \in \mathbb{N}$ together with the bound

$$|f(n)| \ll (e-1)^{\alpha n}$$

for some $\alpha < 1$, then f is a polynomial map. Ruzsa also conjectured that the same result should hold with $e-1$ replaced by e , and some progress on this conjecture has been made by Zannier [16].

Viewed more broadly, Conjecture 1.7 asserts that, if a function f has some special form when reduced modulo p for infinitely many primes p , then f itself must have a special form. We remark that, in other contexts, one may find results of this type; see for instance [8, Theorem 4, pp. 329–330].

4. HEURISTICS

We will now provide a probabilistic argument to support Conjecture 1.7. We begin with some preliminary observations.

Lemma 4.1. *Suppose that $f : \mathbb{Q} \rightarrow \mathbb{Q}$ is a function for which $|S_f| = \infty$. If there is an exponent $k \in \mathbb{Z}$ and a constant C for which $f(q) \in \{q^k, -q^k\}$ for all primes $q \geq C$, then $f(\alpha) = \alpha^k$ for all $\alpha \in \mathbb{Q}$.*

Proof. By Lemma 3.1, $f(\mathbb{Q}^\times) \subseteq \mathbb{Q}^\times$ and f is completely multiplicative, upon which it follows that $f(-1) \in \{1, -1\}$. Thus,

$$\begin{aligned} \forall \alpha \in \mathbb{Q}^\times, \quad f(\alpha) &= f(\text{sgn}(\alpha)) \cdot f(|\alpha|) \\ &= \pm f(|\alpha|), \end{aligned} \tag{13}$$

where $\text{sgn}(\alpha) := \alpha/|\alpha|$ denotes the sign of α . One sees that $f(\alpha)$ is determined by $f(\text{sgn}(\alpha))$ and its restriction

$$f : \mathbb{Q}_+^\times \rightarrow \mathbb{Q}^\times$$

to \mathbb{Q}_+^\times . Assuming that $f(q) = \pm q^k$ for some $k \in \mathbb{Z}$ and all primes $q \geq C$, then define

$$\mu : \mathbb{Q}_+^\times \rightarrow \mathbb{Q}^\times, \quad \mu(\alpha) := \frac{f(\alpha)}{\alpha^k}.$$

One checks that

$$S_f \subseteq S_\mu, \tag{14}$$

and also that

$$\mu(\{q \text{ prime}; q \geq C\}) \subseteq \{\pm 1\}.$$

Either there exists a constant C_1 for which $\mu(\{q \text{ prime}; q \geq C_1\}) = \{1\}$, or for each constant C_1 one has $\mu(\{q \text{ prime}; q \geq C_1\}) = \{1, -1\}$ (since f_p is a homomorphism, one cannot have $\mu(\{q \text{ prime}; q \geq C_1\}) = \{-1\}$). In the first case, by taking a large prime q which is a primitive root modulo p , one finds that $k_p = k$ for each $p \in S_f$. Thus for any $\alpha \in \mathbb{Q}_+^\times$, $f(\alpha) - \alpha^k$ is divisible by infinitely many primes $p \in S_f$, and so $f(\alpha) = \alpha^k$.

If on the other hand $\mu(\{q \text{ prime}; q \geq C_1\}) = \{1, -1\}$ for any constant C_1 , then for each $p \in S_\mu$ and each prime q which is large enough,

$$\mu(q) = \left(\frac{q}{p}\right),$$

the Legendre symbol at p . If there are distinct primes $p_1, p_2 \in S_\mu$, then by Dirichlet's theorem on primes in arithmetic progressions, one may find a prime q with

$$\left(\frac{q}{p_1}\right) \neq \left(\frac{q}{p_2}\right),$$

a contradiction. Thus, in this case $|S_\mu| \leq 1$, contradicting (14). Thus, we see that

$$\forall \alpha \in \mathbb{Q}_+^\times, \quad f(\alpha) = \alpha^k.$$

It follows from (13) that

$$\forall \alpha \in \mathbb{Q}^\times, \quad f(\alpha) = \begin{cases} \alpha^k \\ \text{sgn}(\alpha)\alpha^k, \end{cases} \quad \text{or}$$

according to whether or not $f(-1) = (-1)^k$. If $f(\alpha) = \text{sgn}(\alpha)\alpha^k$, then

$$\text{sgn}(\alpha) = \frac{f(\alpha)}{\alpha^k},$$

and as before we conclude that $S_f \subseteq S_{\text{sgn}}$, which contradicts the fact that $S_{\text{sgn}} = \{2\}$. Therefore $f(\alpha) = \alpha^k$ for every $\alpha \in \mathbb{Q}^\times$, finishing the proof of the lemma. \square

Corollary 4.2. *Suppose that $f : \mathbb{Q} \rightarrow \mathbb{Q}$ satisfies $|S_f| = \infty$. Then either f is a global power map, or for each $L \in \mathbb{N}$, one may find a set*

$$\mathfrak{N}_L = \{n_1, n_2, \dots, n_L\} \subseteq \mathbb{N}$$

of L positive square-free integers satisfying

$$\forall n \in \mathfrak{N}_L \quad f(n) \notin n^{\mathbb{Z}} \cup -n^{\mathbb{Z}}.$$

Proof. Suppose that $|S_f| = \infty$ but f is not a global power map. We proceed by induction on L . For the base case $L = 1$, either there exists a prime q for which $f(q) \notin q^{\mathbb{Z}} \cup -q^{\mathbb{Z}}$ (in which case we set $n = q$), or else for each prime q , $f(q) \in \{q^{k_q}, -q^{k_q}\}$ for some exponent $k_q \in \mathbb{Z}$. In the latter case, provided f is not a global power map, then by Lemma 4.1 one may find two primes q_1 and q_2 for which $k_{q_1} \neq k_{q_2}$. By Lemma 3.1, f must be completely multiplicative, and thus $f(q_1 q_2) \notin (q_1 q_2)^{\mathbb{Z}} \cup -(q_1 q_2)^{\mathbb{Z}}$, so in this case we may set $n = q_1 q_2$. For the induction step, we reason the same way: having constructed \mathfrak{N}_{L-1} , either there exists a prime q larger than any $n \in \mathfrak{N}_{L-1}$ for which $f(q) \notin q^{\mathbb{Z}} \cup -q^{\mathbb{Z}}$ (in which case we set $\mathfrak{N}_L := \mathfrak{N}_{L-1} \cup \{q\}$) or else for each prime q larger than any $n \in \mathfrak{N}_{L-1}$, $f(q) \in \{q^{k_q}, -q^{k_q}\}$. In the second case, by Lemma 4.1 we may find two primes q_1 and q_2 , each larger than any $n \in \mathfrak{N}_{L-1}$ and for which $k_{q_1} \neq k_{q_2}$, and we put $\mathfrak{N}_L := \mathfrak{N}_{L-1} \cup \{q_1 q_2\}$. \square

Now suppose that $f : \mathbb{Q} \rightarrow \mathbb{Q}$ is not a global power map, but nevertheless S_f is infinite. We presently apply probabilistic reasoning to deduce a (heuristic) contradiction. Applying Corollary 4.2 with $L = 3$, we may find three natural numbers $n_1, n_2, n_3 \in \mathbb{N}$ such that for each $i \in \{1, 2, 3\}$, $f(n_i) \notin n_i^{\mathbb{Z}} \cup -n_i^{\mathbb{Z}}$. Consider the rational vectors

$$\mathbf{n} := (n_1, n_2, n_3) \in (\mathbb{Q}^\times)^3 \quad \text{and} \quad f(\mathbf{n}) := (f(n_1), f(n_2), f(n_3)) \in (\mathbb{Q}^\times)^3$$

and define the sets $\Omega_{\mathbf{n}} \subseteq (\mathbb{Q}^\times)^3$, $\Omega_{\mathbf{n}}(p) \subseteq \mathbb{F}_p^3$ by

$$\begin{aligned} \Omega_{\mathbf{n}} &:= \{(\varepsilon_1 n_1^k, \varepsilon_2 n_2^k, \varepsilon_3 n_3^k) : k \in \mathbb{Z}, \varepsilon_i \in \{\pm 1\}\} \subseteq (\mathbb{Q}^\times)^3 \\ \Omega_{\mathbf{n}}(p) &:= \{(\hat{n}_1^k, \hat{n}_2^k, \hat{n}_3^k) : k \in \mathbb{Z}/(p-1)\mathbb{Z}\} \subseteq \mathbb{F}_p^3. \end{aligned}$$

By construction, we have that

$$f(\mathbf{n}) \notin \Omega_{\mathbf{n}}. \tag{15}$$

For an arbitrary prime p for which $\mathbf{n}, f(\mathbf{n}) \in (\mathbb{Z}_{(p)}^\times)^3$, we consider the reduction $f(\mathbf{n}) \pmod{p} \in (\mathbb{F}_p^\times)^3$. We evidently have

$$p \in S_f \implies f(\mathbf{n}) \pmod{p} \in \Omega_{\mathbf{n}}(p) \cap (\mathbb{F}_p^\times)^3. \tag{16}$$

Thus for any prime p , we are motivated to ask how likely it is that

$$f(\mathbf{n}) \pmod{p} \in \Omega_{\mathbf{n}}(p) \cap (\mathbb{F}_p^\times)^3. \tag{17}$$

By virtue of (15), it is reasonable to expect $f(\mathbf{n})$ to behave like a random vector¹ in $(\mathbb{F}_p^\times)^3$, at least with respect to lying in $\Omega_{\mathbf{n}}(p) \cap (\mathbb{F}_p^\times)^3$. The heuristic probability that (17) occurs is thus

$$\text{Prob}(f(\mathbf{n}) \pmod{p} \in \Omega_{\mathbf{n}}(p) \cap (\mathbb{F}_p^\times)^3) \approx \frac{|\Omega_{\mathbf{n}}(p) \cap (\mathbb{F}_p^\times)^3|}{|(\mathbb{F}_p^\times)^3|} \leq \frac{(p-1)}{(p-1)^3}.$$

¹Note that, if $f(\mathbf{n}) \in \Omega_{\mathbf{n}}$, then $f(\mathbf{n}) \pmod{p} \in \Omega_{\mathbf{n}}(p)$ for infinitely many primes p . Indeed, for any p satisfying $\left(\frac{n_i}{p}\right) = \varepsilon_i$ for $i \in \{1, 2, 3\}$, one has $f(\mathbf{n}) \pmod{p} \in \Omega_{\mathbf{n}}(p)$.

Thus, by (16), the “event” $p \in S_f$ should occur with probability no greater than $\frac{1}{(p-1)^2}$, and so it is expected that

$$|\{p \in S_f; p \leq X\}| \leq \sum_{p \leq X} \frac{1}{(p-1)^2}.$$

Since the right hand side is uniformly bounded in X , we expect S_f to be finite, contradicting our assumption that S_f is infinite. This leads us to Conjecture 1.7.

5. PROOF OF MAIN THEOREM

The rest of the paper is devoted to a proof of Theorem 1.9. We begin by observing that, for any parameters $0 \leq Y < Z$, one may bound the quantity $|S_f(x)|$ by two sums:

$$|S_f(x)| \leq \sum_{\substack{p \leq x \\ \forall \ell \in [Y, Z), \\ p \not\equiv 1 \pmod{\ell}}} 1 + \sum_{Y \leq \ell < Z} \sum_{\substack{p \in S_f(x) \\ p \equiv 1 \pmod{\ell}}} 1. \quad (18)$$

We will eventually choose $Y = Y(x)$ and $Z = Z(x)$ appropriately so as to bound each of these sums.

The main ingredient in our proof is an effective version of the Chebotarev density theorem, which will be discussed in general in Section 5.1. It will be applied in the context of cyclotomic extensions to handle the first sum, and in the context of Kummer extensions to handle the second sum. The former “cyclotomic part” forms the content of Sections 5.3 and 5.4, while the latter “Kummer extension” part comprises Sections 5.5 and 5.7.

5.1. Effective Chebotarev density. An effective version of the Chebotarev density theorem was first proved by Lagarias and Odlyzko [9] and further refined by Serre [12]. We will now describe the theorem precisely in the form we will use it.

The Chebotarev density theorem gives an asymptotic formula for the number of primes $p \leq x$ for which the associated Frobenius automorphism has a prescribed action on a given fixed number field. More precisely, let K be a number field which is Galois over \mathbb{Q} with Galois group $G := \text{Gal}(K/\mathbb{Q})$ and discriminant d_K . Furthermore, fix any subset $\mathcal{C} \subseteq G$ satisfying

$$\forall \sigma \in G, \quad \sigma \mathcal{C} \sigma^{-1} = \mathcal{C}. \quad (19)$$

For any rational prime p which doesn’t divide d_K , let $\text{Frob}_p \subseteq G$ denote the conjugacy class in G of the Frobenius automorphism $\text{Frob}_{\mathfrak{p}}$ attached to any prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ lying over $p\mathbb{Z}$. By (19), either $\text{Frob}_p \subseteq \mathcal{C}$ or $\text{Frob}_p \cap \mathcal{C} = \emptyset$, and we consider the counting function

$$\pi(x; K/\mathbb{Q}, \mathcal{C}) := |\{p \leq x; p \nmid d_K \text{ and } \text{Frob}_p \subseteq \mathcal{C}\}|.$$

The Chebotarev density theorem asserts that, as $x \rightarrow \infty$, one has

$$\pi(x; K/\mathbb{Q}, \mathcal{C}) \sim \frac{|\mathcal{C}|}{|G|} \pi(x).$$

We will require the following effective version, which bounds the error term in this asymptotic in terms of data attached to the number field K .

Theorem 5.1. (*Effective Chebotarev Theorem*) *There exist absolute positive constants c_1 and c_2 (with c_1 effective) such that, if $x \geq 2$ and*

$$\sqrt{\frac{\log x}{[K:\mathbb{Q}]}} \geq c_2 \max \left\{ \log |d_K|, |d_K|^{1/[K:\mathbb{Q}]} \right\}, \quad (20)$$

then

$$\pi(x; K/\mathbb{Q}, \mathcal{C}) = \frac{|\mathcal{C}|}{|G|} \pi(x) + O \left(|\mathcal{C}| \cdot x \cdot \exp \left(-c_1 \sqrt{\frac{\log x}{[K:\mathbb{Q}]}} \right) \right).$$

5.2. Bounding each sum in (18). We will now state two propositions which bound respectively the first and second sums occurring on the right-hand side of (18).

First observe that, by the prime number theorem, one has

$$\sum_{\ell \leq Z} \log \ell \sim Z \quad (Z \rightarrow \infty),$$

and consequently there exists a positive real constant M for which

$$\forall Z \geq 2, \quad \prod_{\ell \leq Z} \ell \leq e^{MZ}. \quad (21)$$

In fact, one can take $M = \log 4$ (see [14, Theorem 4, p. 11]).

Proposition 5.2. *Assume that*

$$2 \leq Y \leq Z \leq \frac{1}{3M+1} \cdot \log \log x,$$

where M is as in (21). Then, for Z sufficiently large, one has

$$\sum_{\substack{p \leq x \\ \forall \ell \in [Y, Z], \\ p \not\equiv 1 \pmod{\ell}}} 1 \ll \frac{\log Y}{\log Z} \cdot \pi(x),$$

with an absolute implied constant.

Our next proposition bounds the second sum in (18).

Proposition 5.3. *Suppose that $f : \mathbb{Q} \rightarrow \mathbb{Q}$ is not a global power map. There exists constants $a_f, b_f > 0$ so that, provided*

$$a_f \leq Y \leq Z \leq \left(\frac{\log x}{(6c_2 \log \log x)^2} \right)^{1/15},$$

(where c_2 is the constant appearing in (20)) then one has

$$\sum_{Y \leq \ell < Z} \sum_{\substack{p \in S_f(x) \\ p \equiv 1 \pmod{\ell}}} 1 \ll \frac{1}{Y \log Y} \cdot \pi(x) + b_f,$$

with an absolute implied constant.

Inserting the results of Propositions 5.2 and 5.3 into (18) and putting

$$Y = \frac{\log \log \log x}{(\log \log \log x)^2}, \quad Z = \frac{1}{3M+1} \cdot \log \log x,$$

we see that Theorem 1.9 follows.

The remainder of the paper is devoted to proving the two propositions. To prove Proposition 5.2, we will apply Theorem 5.1 with K equal to a cyclotomic field:

$$K = \mathbb{Q}(\zeta_{n_{Y,Z}}) \quad \left(n_{Y,Z} := \prod_{Y \leq \ell < Z} \ell \right).$$

To prove Proposition 5.3, we will apply the same theorem with K equal to a field extension of the form

$$K = \mathbb{Q} \left(\zeta_\ell, n_1^{1/\ell}, n_2^{1/\ell}, f(n_1)^{1/\ell}, f(n_2)^{1/\ell} \right),$$

for appropriately chosen $n_1, n_2 \in \mathbb{N}$.

5.3. Cyclotomic extensions. We will now state a few preparatory lemmas about the discriminant and Frobenius automorphism in cyclotomic fields.

Lemma 5.4. *Let $n \geq 1$ be a positive integer and let $K = \mathbb{Q}(\zeta_n)$. The discriminant d_K is given by*

$$d_K = (-1)^{\varphi(n)/2} \cdot \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}.$$

In particular

$$|d_K| \leq n^{\varphi(n)},$$

and a prime number p is ramified in $\mathbb{Q}(\zeta_n)$ if and only if p divides n .

Proof. This is classical; see for instance [15, Proposition 2.7, p. 12]. \square

Any prime p not dividing d_K is unramified in K , and given a prime ideal $\mathfrak{P} \subseteq \mathcal{O}_K$ lying above $p\mathbb{Z} \subseteq \mathbb{Z}$, we may consider the Frobenius automorphism at \mathfrak{P} in $\text{Gal}(K/\mathbb{Q})$, which we denote by

$$\text{Frob}_{\mathfrak{P}} \in \text{Gal}(K/\mathbb{Q}).$$

When K is abelian over \mathbb{Q} , the automorphism $\text{Frob}_{\mathfrak{P}}$ is independent of the choice of \mathfrak{P} over p . We will thus denote it by Frob_p in this case, since it depends only on p . Furthermore, when $K = \mathbb{Q}(\zeta_n)$, one has the following result, which identifies $\text{Frob}_p \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, under the canonical group isomorphism

$$\begin{aligned} \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) &\leftrightarrow (\mathbb{Z}/n\mathbb{Z})^\times \\ (\zeta_n &\mapsto \zeta_n^a) \mapsto a. \end{aligned} \tag{22}$$

Lemma 5.5. *If p does not divide n , then p is unramified in $\mathbb{Q}(\zeta_n)$. Furthermore, under the isomorphism (22), the Frobenius automorphism $\text{Frob}_p \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is identified with $p \in (\mathbb{Z}/n\mathbb{Z})^\times$.*

Proof. See for instance [15, Lemma 2.12], and the discussion thereafter. \square

5.4. Proof of Proposition 5.2. We are now ready to prove Proposition 5.2. Notice that, by Lemmas 5.4 and 5.5, one has that for any prime p ,

$$\forall \ell \in [Y, Z], p \not\equiv 1 \pmod{\ell} \implies p \in [Y, Z] \text{ or } \text{Frob}_p \in \mathcal{C},$$

where, under $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ and the isomorphism

$$(\mathbb{Z}/n_{Y,Z}\mathbb{Z})^\times \simeq \prod_{Y \leq \ell < Z} (\mathbb{Z}/\ell\mathbb{Z})^\times$$

of the Chinese remainder theorem,

$$\mathcal{C} := \prod_{Y \leq \ell < Z} ((\mathbb{Z}/\ell\mathbb{Z})^\times - \{1\}).$$

Thus we have

$$\sum_{\substack{p \leq x \\ \forall \ell \in [Y, Z], \\ p \not\equiv 1 \pmod{\ell}}} 1 \leq \pi(x; K/\mathbb{Q}, \mathcal{C}) + \pi(Z). \tag{23}$$

We will now apply Theorem 5.1 to bound $\pi(x; K/\mathbb{Q}, \mathcal{C})$. We begin by using Lemma 5.4 to establish a bound for Z sufficient to guarantee that condition (20) is satisfied.

Note that

$$[K : \mathbb{Q}] = \varphi(n_{Y,Z}) \leq n_{Y,Z} \leq e^{MZ},$$

by (21). Thus,

$$|d_K|^{1/[K:\mathbb{Q}]} \leq (n_{Y,Z}^{\varphi(n_{Y,Z})})^{1/\varphi(n_{Y,Z})} \leq e^{MZ},$$

and also

$$\log |d_K| \leq \varphi(n_{Y,Z}) \log n_{Y,Z} \leq e^{MZ} \cdot (MZ).$$

We therefore have the following corollary of Lemma 5.4.

Corollary 5.6. For $K = \mathbb{Q}(\zeta_{n_{Y,Z}})$ with $n_{Y,Z} := \prod_{Y \leq \ell < Z} \ell$, one has

$$\max \left\{ \log |d_K|, |d_K|^{1/[K:\mathbb{Q}]} \right\} \leq MZe^{MZ}.$$

In particular, if

$$Z \leq \frac{1}{3M+1} \log \log x, \quad (24)$$

then for x large enough, (20) is satisfied in this case.

Returning to (23), note that

$$|\mathcal{C}| = \prod_{Y \leq \ell < Z} (\ell - 2) = [K:\mathbb{Q}] \cdot \prod_{Y \leq \ell < Z} \left(1 - \frac{1}{\ell - 1}\right) \ll [K:\mathbb{Q}] \cdot \frac{\log Y}{\log Z},$$

by Merten's theorem. Furthermore, (24) implies that

$$e^{MZ} < (\log x)^{1/3}.$$

Thus, assuming (24), Theorem 5.1 implies

$$\begin{aligned} \pi(x; K/\mathbb{Q}, \mathcal{C}) &= \frac{|\mathcal{C}|}{[K:\mathbb{Q}]} \cdot \pi(x) + O \left(|\mathcal{C}| \cdot x \cdot \exp \left(-c_1 \sqrt{\frac{\log x}{[K:\mathbb{Q}]}} \right) \right) \\ &\ll \frac{\log Y}{\log Z} \cdot \pi(x) + e^{MZ} \cdot x \cdot \exp \left(-c_1 \sqrt{\frac{\log x}{e^{Mz}}} \right) \\ &\leq \frac{\log Y}{\log Z} \cdot \pi(x) + (\log x)^{1/3} \cdot x \cdot \exp \left(-c_1 (\log x)^{1/3} \right). \end{aligned} \quad (25)$$

For any $A > 0$ one has

$$\exp \left(-c_1 (\log x)^{1/3} \right) \ll_A \frac{1}{(\log x)^A}, \quad (26)$$

so by inserting (25) into (23) we conclude that

$$\sum_{\substack{p \leq x \\ \forall \ell \in [Y, Z), \\ p \not\equiv 1 \pmod{\ell}}} 1 \ll \frac{\log Y}{\log Z} \cdot \pi(x) + \frac{x}{(\log x)^2} + \frac{Z}{\log Z}.$$

In light of (24) and the prime number theorem, we have

$$\frac{Z}{\log Z} \ll \log \log x \ll \frac{x}{(\log x)^2} \ll \frac{x}{\log x \log \log \log x} \ll \frac{\log Y}{\log Z} \cdot \pi(x)$$

and so this finishes the proof of Proposition 5.2.

5.5. Kummer extensions. To prove Proposition 5.3, we will apply Theorem 5.1 to a field extension of the form

$$K = \mathbb{Q} \left(\zeta_\ell, n_1^{1/\ell}, n_2^{1/\ell}, f(n_1)^{1/\ell}, f(n_2)^{1/\ell} \right),$$

for appropriately chosen $n_1, n_2 \in \mathbb{N}$. In order to do this, we need some control on the Galois group $\text{Gal}(K/\mathbb{Q})$ in this case. If f is a global power map then $K = \mathbb{Q}(\zeta_\ell, n_1^{1/\ell}, n_2^{1/\ell})$, and one cannot deduce the result of Proposition 5.3. In case f is not a global power map but nevertheless $|S_f| = \infty$, then it is still not immediately clear that one may find $n_1, n_2 \in \mathbb{N}$ for which $[K:\mathbb{Q}(\zeta_\ell)] = \ell^4$ for all primes ℓ which are large enough, but we show that one may achieve $[K:\mathbb{Q}(\zeta_\ell)] \geq \ell^3$ for $\ell \gg_f 1$, which suffices for our purposes (see Corollary 5.12 below).

We begin by reviewing some fundamental facts about Kummer extensions. For any integers $m \geq 0$ and $n \geq 1$ and vector $\mathbf{c} = (c_1, c_2, \dots, c_m) \in (\mathbb{Q}^\times)^m$, we will call a number field of the form

$$K = \mathbb{Q}(\zeta_n, \mathbf{c}^{1/n}) := \mathbb{Q}(\zeta_n, c_1^{1/n}, c_2^{1/n}, \dots, c_m^{1/n})$$

a *Kummer extension* (in case $m = 0$, we interpret this as $\mathbb{Q}(\zeta_n, \mathbf{c}^{1/n}) := \mathbb{Q}(\zeta_n)$). In our application, we will deal exclusively with the case where $n = \ell$ is an odd prime number, and we begin by describing the associated Galois group. Consider the group

$$(\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes (\mathbb{Z}/\ell\mathbb{Z})^m,$$

where the semi-direct product is defined via the multiplicative action of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ on $(\mathbb{Z}/\ell\mathbb{Z})^m$, or explicitly

$$(a_1, \mathbf{b}_1) \cdot (a_2, \mathbf{b}_2) = (a_1 a_2, \mathbf{b}_2 + a_2 \mathbf{b}_1),$$

where $\mathbf{b}_i \in (\mathbb{Z}/\ell\mathbb{Z})^m$. (Equivalently, the embedding

$$(\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes (\mathbb{Z}/\ell\mathbb{Z})^m \hookrightarrow GL_{m+1}(\mathbb{Z}/\ell\mathbb{Z})$$

$$(a, \mathbf{b}) \mapsto \begin{pmatrix} a & 0 \\ \mathbf{b} & I \end{pmatrix},$$

where I denotes the $m \times m$ identity matrix, allows one to regard $(\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes (\mathbb{Z}/\ell\mathbb{Z})^m$ as a subgroup of $GL_{m+1}(\mathbb{Z}/\ell\mathbb{Z})$. There is an embedding of groups²

$$\text{Gal}(\mathbb{Q}(\zeta_\ell, \mathbf{c}^{1/\ell})/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes (\mathbb{Z}/\ell\mathbb{Z})^m$$

$$\begin{pmatrix} \zeta_\ell & \mapsto & \zeta_\ell^a \\ c_i^{1/\ell} & \mapsto & c_i^{1/\ell} \cdot \zeta_\ell^{b_i} \end{pmatrix} \mapsto (a, \mathbf{b}), \quad (27)$$

where $\mathbf{b} = (b_1, b_2, \dots, b_m)$. What is the image of this embedding? In general, the image depends on whether (and to what extent) there exist multiplicative relations

$$\mathbf{c}^{\mathbf{d}/\ell} := \prod_{i=1}^m (c_i^{1/\ell})^{d_i} \in \mathbb{Q}^\times, \quad (28)$$

where in the above, $\mathbf{d} = (d_1, d_2, \dots, d_m) \in (\mathbb{Z}/\ell\mathbb{Z})^m$. In our application, we will need to understand the image of this embedding, even in the case where nontrivial relations such as (28) exist.

Let $V_{\mathbf{c}}(\ell)$, respectively $V_{\mathbf{c}}^\perp(\ell)$ denote the $\mathbb{Z}/\ell\mathbb{Z}$ -vector subspaces

$$V_{\mathbf{c}}(\ell) := \{\mathbf{d} \in (\mathbb{Z}/\ell\mathbb{Z})^m : \text{the relation (28) holds}\}$$

$$V_{\mathbf{c}}^\perp(\ell) := \{\mathbf{b} \in (\mathbb{Z}/\ell\mathbb{Z})^m : \forall \mathbf{d} \in V_{\mathbf{c}}(\ell), \sum_{i=1}^m b_i d_i \equiv 0 \pmod{\ell}\}. \quad (29)$$

It follows from (28) and (29) that the image of the embedding (27) is equal to the subgroup

$$(\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes V_{\mathbf{c}}^\perp(\ell) \subseteq (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes (\mathbb{Z}/\ell\mathbb{Z})^m.$$

The following lemma summarizes our discussion, and uses the notation

$$d_{\mathbf{c}} := \dim_{\mathbb{Z}/\ell\mathbb{Z}} V_{\mathbf{c}}^\perp(\ell) \in \mathbb{N} \cup \{0\}. \quad (30)$$

Lemma 5.7. *The function (27) gives an isomorphism of groups*

$$\text{Gal}(\mathbb{Q}(\zeta_\ell, \mathbf{c}^{1/\ell})/\mathbb{Q}) \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes V_{\mathbf{c}}^\perp(\ell).$$

Furthermore (after possibly re-labelling indices) we have that

$$\mathbb{Q}(\zeta_\ell, c_1^{1/\ell}, c_2^{1/\ell}, \dots, c_m^{1/\ell}) = \mathbb{Q}(\zeta_\ell, c_1^{1/\ell}, c_2^{1/\ell}, \dots, c_d^{1/\ell}),$$

where $d = d_{\mathbf{c}}$ is defined by (30). This choice of d is the smallest possible³. In particular, one has

$$\text{Gal}(\mathbb{Q}(\zeta_\ell, c_1^{1/\ell}, c_2^{1/\ell}, \dots, c_m^{1/\ell})/\mathbb{Q}) = \text{Gal}(\mathbb{Q}(\zeta_\ell, c_1^{1/\ell}, c_2^{1/\ell}, \dots, c_d^{1/\ell})/\mathbb{Q})$$

$$\simeq (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes (\mathbb{Z}/\ell\mathbb{Z})^d.$$

²Here we are interpreting $\text{Gal}(\mathbb{Q}(\zeta_\ell, \mathbf{c}^{1/\ell})/\mathbb{Q})$ as operating on the *right*.

³In case $d = 0$, we make the interpretation $\mathbb{Q}(\zeta_\ell, c_1^{1/\ell}, c_2^{1/\ell}, \dots, c_d^{1/\ell}) := \mathbb{Q}(\zeta_\ell)$ and $(\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes (\mathbb{Z}/\ell\mathbb{Z})^d := (\mathbb{Z}/\ell\mathbb{Z})^\times$.

Proof. Let $B \subseteq \mathbb{Q}^\times$ be the multiplicative subgroup generated by $(\mathbb{Q}^\times)^\ell$ and $\{c_i : 1 \leq i \leq m\}$. In [10, Theorem 8.1, p. 294–295] it is shown that

$$\text{Gal}(\mathbb{Q}(\zeta_\ell, \mathbf{c}^{1/\ell})/\mathbb{Q}(\zeta_\ell)) \simeq \frac{B}{(\mathbb{Q}^\times)^\ell}.$$

Noting that, under $\mathbf{c}^{\mathbf{n}} \pmod{\ell} \mapsto \mathbf{n} \pmod{\ell}$, one has

$$\frac{B}{(\mathbb{Q}^\times)^\ell} \simeq \frac{(\mathbb{Z}/\ell\mathbb{Z})^m}{V_{\mathbf{c}}(\ell)} \simeq V_{\mathbf{c}}^\perp(\ell),$$

one concludes that $\text{Gal}(\mathbb{Q}(\zeta_\ell, \mathbf{c}^{1/\ell})/\mathbb{Q}(\zeta_\ell)) \simeq V_{\mathbf{c}}^\perp(\ell)$, and the conclusion of the lemma follows. \square

In our proof of Proposition 5.3, it will become important to know that the subspace $V_{\mathbf{c}}^\perp(\ell) \subseteq (\mathbb{Z}/\ell\mathbb{Z})^m$ is not too small, which motivates the following lemma. Let us define the \mathbb{Z} -modules $M_{\mathbf{c}}$ and $M_{\mathbf{c},\ell}$ by

$$\begin{aligned} M_{\mathbf{c}} &:= \{\mathbf{n} \in \mathbb{Z}^m : \mathbf{c}^{\mathbf{n}} \in \{\pm 1\}\}, \\ M_{\mathbf{c},\ell} &:= \{\mathbf{n} \in \mathbb{Z}^m : \mathbf{c}^{\mathbf{n}} \in (\mathbb{Q}^\times)^\ell\} \\ &= \{\mathbf{n} \in \mathbb{Z}^m : \mathbf{n} \pmod{\ell} \in V_{\mathbf{c}}(\ell)\}. \end{aligned} \tag{31}$$

Note that, if ℓ is an odd prime, then $M_{\mathbf{c}} \subseteq M_{\mathbf{c},\ell}$.

Lemma 5.8. *Let $m \geq 1$ and $\mathbf{c} \in (\mathbb{Q}^\times)^m$, and let ℓ be an odd prime number. Then*

$$[\mathbb{Q}(\zeta_\ell, \mathbf{c}^{1/\ell}) : \mathbb{Q}(\zeta_\ell)] < \ell^m \iff M_{\mathbf{c},\ell} \neq \{\mathbf{0}\}.$$

Proof. Using the previous lemma and (31), one sees that

$$[\mathbb{Q}(\zeta_\ell, \mathbf{c}^{1/\ell}) : \mathbb{Q}(\zeta_\ell)] < \ell^m \iff V_{\mathbf{c}}(\ell) \neq \{\mathbf{0}\} \iff M_{\mathbf{c},\ell} \neq \{\mathbf{0}\}.$$

\square

Now let S be any set of odd primes. One concludes from the definitions that

$$|S| = \infty \implies M_{\mathbf{c}} = \bigcap_{\ell \in S} M_{\mathbf{c},\ell}. \tag{32}$$

More is true.

Lemma 5.9. *Let S be a set of odd prime numbers. If $|S| = \infty$ then*

$$M_{\mathbf{c}} \neq \{\mathbf{0}\} \iff \forall \ell \in S, M_{\mathbf{c},\ell} \neq \{\mathbf{0}\}.$$

Proof. The “ \implies ” direction is clear from (32). For the converse, let

$$\begin{aligned} R &:= \{\text{primes } p : v_p(c_i) \neq 0 \text{ for some } i \in \{1, 2, \dots, m\}\} \\ &= \{p_1, p_2, \dots, p_r\}, \end{aligned}$$

where $r := |R|$, and define the vectors $\mathbf{e}_j \in \mathbb{Z}^R$ by

$$\begin{aligned} c_j &:= \prod_{p \in R} p^{\mathbf{e}_j(p)} \\ &= \prod_{i=1}^r p_i^{\mathbf{e}_{i,j}}. \end{aligned}$$

Furthermore, consider the $r \times m$ integer matrix

$$\mathbf{E}_{\mathbf{c}} := (\mathbf{e}_1 \quad \mathbf{e}_2 \quad \dots \quad \mathbf{e}_m) \in M_{r \times m}(\mathbb{Z})$$

whose columns are the vectors \mathbf{e}_j . Note that, for any vector $\mathbf{n} \in \mathbb{Z}^m$,

$$\begin{aligned} \mathbf{c}^{\mathbf{n}} \in \{\pm 1\} &\iff \mathbf{E}_{\mathbf{c}} \cdot \mathbf{n} = \mathbf{0}, \\ \mathbf{c}^{\mathbf{n}} \in (\mathbb{Q}^\times)^\ell &\iff \mathbf{E}_{\mathbf{c}} \cdot \mathbf{n} \equiv \mathbf{0} \pmod{\ell}, \end{aligned}$$

so in particular

$$M_{\mathbf{c}} = \{\mathbf{n} \in \mathbb{Z}^m : \mathbf{E}_{\mathbf{c}} \cdot \mathbf{n} = \mathbf{0}\}, \quad \text{and} \\ M_{\mathbf{c},\ell} = \{\mathbf{n} \in \mathbb{Z}^m : \mathbf{E}_{\mathbf{c}} \cdot \mathbf{n} \equiv \mathbf{0} \pmod{\ell}\}.$$

Note that, if $r < m$ then necessarily $\ker \mathbf{E}_{\mathbf{c}}$ has dimension at least one, so $M_{\mathbf{c}} \neq \{\mathbf{0}\}$ in this case. In case $r \geq m$, let $w := \binom{r}{m} \in \mathbb{N}$ and let $\Delta_{\mathbf{c}} \in \mathbb{Z}^w$ be the vector of determinants of all $m \times m$ sub-matrices of $\mathbf{E}_{\mathbf{c}}$. One has

$$M_{\mathbf{c}} \neq \{\mathbf{0}\} \iff \Delta_{\mathbf{c}} = \mathbf{0}, \\ M_{\mathbf{c},\ell} \neq \{\mathbf{0}\} \iff \Delta_{\mathbf{c}} \equiv \mathbf{0} \pmod{\ell}. \quad (33)$$

Thus,

$$\forall \ell \in S, M_{\mathbf{c},\ell} \neq \{\mathbf{0}\} \Rightarrow \forall \ell \in S, \Delta_{\mathbf{c}} \equiv \mathbf{0} \pmod{\ell} \Rightarrow \Delta_{\mathbf{c}} = \mathbf{0} \Rightarrow M_{\mathbf{c}} \neq \{\mathbf{0}\},$$

proving the lemma. \square

The next lemma will be useful for making sure that our Kummer extensions are not too small.

Lemma 5.10. *Let $m \geq 1$ and $\mathbf{c} \in (\mathbb{Q}^\times)^m$, and let S be an infinite set of odd prime numbers. One has*

$$\forall \ell \in S, \left[\mathbb{Q} \left(\zeta_\ell, \mathbf{c}^{1/\ell} \right) : \mathbb{Q}(\zeta_\ell) \right] < \ell^m \iff M_{\mathbf{c}} \neq \{\mathbf{0}\}.$$

Proof. Apply Lemmas 5.8 and 5.9. \square

Remark 5.11. Suppose that $\mathbf{c} \in (\mathbb{Q}^\times)^m$ and $M_{\mathbf{c}} = \{\mathbf{0}\}$. By (33), we have that $\Delta_{\mathbf{c}} \neq \mathbf{0}$. Thus, writing $\Delta_{\mathbf{c}} =: (\lambda_1, \lambda_2, \dots, \lambda_w)$, we may define $\delta(\mathbf{c}) := 2 \gcd(\lambda_1, \lambda_2, \dots, \lambda_w)$. The proof of Lemma 5.9 shows that

$$\ell \nmid \delta(\mathbf{c}) \implies \left[\mathbb{Q} \left(\zeta_\ell, \mathbf{c}^{1/\ell} \right) : \mathbb{Q}(\zeta_\ell) \right] = \ell^m.$$

The next corollary follows from applying Lemma 5.10 with $\mathbf{c} = (n_1, n_2, f(n_1)) \in (\mathbb{Q}^\times)^3$ with $n_1, n_2 \in \mathbb{N}$ chosen in accordance with Corollary 4.2. Let us make the following definitions, for $\mathbf{n} = (n_1, n_2) \in \mathbb{N}^2$:

$$\mathbf{c}_{f,\mathbf{n}} := (n_1, n_2, f(n_1)) \in (\mathbb{Q}^\times)^3 \\ \mathcal{N}_f := \{\mathbf{n} \in \mathbb{N}^2 : M_{\mathbf{c}_{f,\mathbf{n}}} = \{\mathbf{0}\}\}.$$

If $\mathbf{n} \in \mathcal{N}_f$, then the vector $\Delta_{\mathbf{c}_{f,\mathbf{n}}} =: (\lambda_1^{(f,\mathbf{n})}, \lambda_2^{(f,\mathbf{n})}, \dots, \lambda_w^{(f,\mathbf{n})}) \in \mathbb{Z}^w$ appearing in the proof of Lemma 5.9 is well-defined and non-zero. We then set

$$\delta_{f,\mathbf{n}} := 2 \gcd(\lambda_1^{(f,\mathbf{n})}, \lambda_2^{(f,\mathbf{n})}, \dots, \lambda_w^{(f,\mathbf{n})}).$$

Corollary 5.12. *Suppose that $f : \mathbb{Q} \rightarrow \mathbb{Q}$ satisfies $|S_f| = \infty$. Then either f is a global power map, or $\mathcal{N}_f \neq \emptyset$. Furthermore, for any $\mathbf{n} = (n_1, n_2) \in \mathcal{N}_f$ and for any odd prime ℓ one has*

$$\ell \nmid \delta_{f,\mathbf{n}} \implies \left[\mathbb{Q} \left(\zeta_\ell, n_1^{1/\ell}, n_2^{1/\ell}, f(n_1)^{1/\ell}, f(n_2)^{1/\ell} \right) : \mathbb{Q}(\zeta_\ell) \right] \geq \ell^3$$

Proof. Let $n \in \mathbb{N}$. By Lemma 5.10, $\left[\mathbb{Q} \left(\zeta_\ell, n^{1/\ell}, f(n)^{1/\ell} \right) : \mathbb{Q}(\zeta_\ell) \right] < \ell^2$ for infinitely many primes ℓ if and only if

$$n^c f(n)^d \in \{\pm 1\} \text{ for some } (c, d) \in \mathbb{Z}^2 - \{(0, 0)\}, \quad (34)$$

and we may as well take c and d to be relatively prime. If n is further assumed to be square-free and greater than 1, then one finds that $d = 1$ in (34), and so this happens if and only if

$$f(n) \in n^{\mathbb{Z}} \cup -n^{\mathbb{Z}}. \quad (35)$$

By Corollary 4.2, one may find a square-free number n for which (35) does not happen. Putting $n_1 := n$ and taking $n_2 = p$ to be any prime for which $v_p(n_1) = v_p(f(n_1)) = 0$, we see that $M_{\mathbf{c}_{f,\mathbf{n}}} = \{\mathbf{0}\}$. Applying Remark 5.11, we see that, for $\ell \nmid \delta_{f,\mathbf{n}}$, one has $[\mathbb{Q}(\zeta_\ell, \mathbf{c}_{f,\mathbf{n}}^{1/\ell}) : \mathbb{Q}(\zeta_\ell)] = \ell^3$, which proves the corollary. \square

The next lemma deals with the absolute discriminant of the field

$$\begin{aligned} K = \mathbb{Q}(\zeta_\ell, \mathbf{c}^{1/\ell}) &:= \mathbb{Q}(\zeta_\ell, c_1^{1/\ell}, c_2^{1/\ell}, \dots, c_m^{1/\ell}) \\ &= \mathbb{Q}(\zeta_\ell, c_1^{1/\ell}, c_2^{1/\ell}, \dots, c_d^{1/\ell}), \end{aligned} \quad (36)$$

where $0 \leq d = d_c \leq m$ is as in (30). Its proof utilizes the following classical formula for relative discriminants.

Lemma 5.13. *Let $F \subseteq L \subseteq K$ be a tower of number fields, let $\Delta_{K/L} \subseteq \mathcal{O}_L$, $\Delta_{K/F} \subseteq \mathcal{O}_F$, and $\Delta_{L/F} \subseteq \mathcal{O}_F$ be the relative discriminants and let $\mathfrak{N}_{L/F} : L^\times \rightarrow F^\times$ the usual norm map. Then one has*

$$\Delta_{K/F} = \mathfrak{N}_{L/F}(\Delta_{K/L}) \Delta_{L/F}^{[K:L]}. \quad (37)$$

Proof. See for instance [5, p. 126]. \square

Lemma 5.14. *Let K be as in (36). Then the absolute discriminant d_K divides*

$$\left(\prod_{i=1}^d \text{Num}(c_i) \text{Den}(c_i) \right)^{(\ell-1)^2 \ell^{d-1}} \ell^{(d+1)(\ell-1)^2 \ell^{d-1}}.$$

Proof. We induct on d . We will apply Lemma 5.13 with $F = \mathbb{Q}$,

$$L = \begin{cases} \mathbb{Q}(\zeta_\ell) & \text{if } d = 1 \\ \mathbb{Q}(\zeta_\ell, c_1^{1/\ell}, c_2^{1/\ell}, \dots, c_{d-1}^{1/\ell}) & \text{if } d > 1 \end{cases}$$

and $K = L(c_d^{1/\ell})$. First note that, for any $\alpha \in \mathcal{O}_K$ satisfying $K = L(\alpha)$, one has

$$\mathfrak{D}(\alpha) \cdot \mathcal{O}_L \subseteq \Delta_{K/L}, \quad (38)$$

where $\mathfrak{D}(\alpha)$ is the square of the determinant of the $\ell \times \ell$ matrix whose (i, j) -th entry is $\sigma_i(\alpha^j)$, where $\{\sigma_0, \sigma_1, \dots, \sigma_{\ell-1}\}$ is the set of embeddings of K into \mathbb{C} fixing L point-wise and $0 \leq j \leq \ell - 1$. Let us abbreviate $c := c_d$. Writing $c = a/b$ in lowest terms, and applying (38) with $\alpha = (ab^{\ell-1})^{1/\ell} = c^{1/\ell}b$ and again with $\alpha = (a^{\ell-1}b)^{1/\ell} = c^{-1/\ell}a$, we conclude that

$$\mathfrak{D}\left((ab^{\ell-1})^{1/\ell}\right) \cdot \mathcal{O}_L + \mathfrak{D}\left((a^{\ell-1}b)^{1/\ell}\right) \cdot \mathcal{O}_L \subseteq \Delta_{K/L}.$$

Now for any integer n , one computes that $\mathfrak{D}(n^{1/\ell}) = n^{\ell-1} \ell^{\ell-2}$. Using this, the greatest common divisor on the left-hand side is readily calculated, showing that

$$(\text{Num}(c) \text{Den}(c))^{\ell-1} \ell^{\ell-2} \mathcal{O}_L \subseteq \Delta_{K/L}.$$

Inserting this information into (37), we find that

$$\Delta_{K/\mathbb{Q}} \text{ divides } (\text{Num}(c) \text{Den}(c))^{(\ell-1)^2 \ell^{d-1}} \ell^{(\ell-2)(\ell-1) \ell^{d-1}} \Delta_{L/\mathbb{Q}}^\ell.$$

Applying the induction hypothesis (or the formula $d_{\mathbb{Q}(\zeta_\ell)} = \pm \ell^{\ell-2}$ of Lemma 5.4 in the base case), the conclusion of Lemma 5.14 now follows. \square

In particular, since $|d_K| \leq \left(\prod_{i=1}^d \text{Num}(c_i) \text{Den}(c_i) \right)^{(\ell-1)^2 \ell^{d-1}} \ell^{(d+1)(\ell-1)^2 \ell^{d-1}}$, we obtain the following corollary. Let us put

$$b_{f, \mathbf{n}} := \left| \prod_{i=1}^2 n_i \text{Num}(f(n_i)) \text{Den}(f(n_i)) \right|.$$

Corollary 5.15. *Suppose $f : \mathbb{Q} \rightarrow \mathbb{Q}$ is any function and let $K = \mathbb{Q}(\zeta_\ell, n_1^{1/\ell}, n_2^{1/\ell}, f(n_1)^{1/\ell}, f(n_2)^{1/\ell})$. Then for any prime ℓ satisfying $[K : \mathbb{Q}(\zeta_\ell)] \geq \ell^3$ and $\log \ell \geq b_{f, \mathbf{n}}$, one has*

$$\max \left\{ \log |d_K|, |d_K|^{1/[K:\mathbb{Q}]} \right\} \leq 6\ell^5 \log \ell.$$

5.6. The Frobenius automorphism in Kummer extensions. We now turn our consideration to the Frobenius automorphism $\text{Frob}_{\mathfrak{P}}$ for a prime ideal $\mathfrak{P} \subseteq \mathcal{O}_K$ lying over $p\mathbb{Z}$, where $K = \mathbb{Q}(\zeta_\ell, c^{1/\ell})$ and $p \equiv 1 \pmod{\ell}$.

We begin by describing the situation when $m = d = 1$, i.e. (dropping subscripts) we have

$$K = K_c := \mathbb{Q}(\zeta_\ell, c^{1/\ell}) \neq \mathbb{Q}(\zeta_\ell) \quad (c \in \mathbb{Q}^\times)$$

and

$$\begin{aligned} \text{Gal}(K_c/\mathbb{Q}) &\simeq (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes \mathbb{Z}/\ell\mathbb{Z} \\ \begin{pmatrix} \zeta_\ell & \mapsto & \zeta_\ell^a \\ c^{1/\ell} & \mapsto & c^{1/\ell} \cdot \zeta_\ell^b \end{pmatrix} &\mapsto (a, b), \end{aligned} \tag{39}$$

The minimal polynomials over \mathbb{Q} of ζ_ℓ and $c^{1/\ell}$, together with their factorizations over $\overline{\mathbb{Q}}$, are given respectively as follows:

$$\begin{aligned} \Phi_\ell(t) &:= \frac{t^\ell - 1}{t - 1} = \prod_{i \in (\mathbb{Z}/\ell\mathbb{Z})^\times} (t - \zeta_\ell^i), \\ t^\ell - c &= \prod_{i \in \mathbb{Z}/\ell\mathbb{Z}} (t - \zeta_\ell^i \cdot c^{1/\ell}). \end{aligned}$$

In our present discussion, we will adopt the standing assumptions that

$$p \equiv 1 \pmod{\ell} \quad \text{and} \quad \text{ord}_p(c) = 0. \tag{40}$$

By Lemmas 5.5 and 5.14, these conditions imply that

$$p \text{ splits completely in } \mathbb{Q}(\zeta_\ell) \quad \text{and} \quad p \text{ is unramified in } K_c.$$

Consider the subgroup $\mu_\ell \subseteq \overline{\mathbb{F}_p}^\times$ of ℓ -th roots of unity. Since $p \equiv 1 \pmod{\ell}$, one can find an element $z \in \mathbb{Z}$ whose reduction \hat{z} modulo p generates μ_ℓ , i.e. we have

$$\langle \hat{z} \rangle = \mu_\ell \subseteq \mathbb{F}_p^\times, \tag{41}$$

and the reductions modulo p of the above minimal polynomials factorize over $\overline{\mathbb{F}_p}$ as

$$\begin{aligned} \Phi_\ell(t) &\equiv \prod_{i \in (\mathbb{Z}/\ell\mathbb{Z})^\times} (t - \hat{z}^i) \pmod{p}, \\ t^\ell - c &\equiv \prod_{i \in \mathbb{Z}/\ell\mathbb{Z}} (t - \hat{z}^i \theta_c) \pmod{p}, \end{aligned}$$

for some $\theta_c \in \overline{\mathbb{F}_p}^\times / \mu_\ell$. Furthermore, one has the prime factorization

$$p\mathcal{O}_{\mathbb{Q}(\zeta_\ell)} = \prod_{i \in (\mathbb{Z}/\ell\mathbb{Z})^\times} \mathfrak{p}_{z,i}, \quad \left(\mathfrak{p}_{z,i} := p\mathcal{O}_{\mathbb{Q}(\zeta_\ell)} + (\zeta_\ell - z^{i*})\mathcal{O}_{\mathbb{Q}(\zeta_\ell)} \right),$$

where i^* denotes an integer satisfying $i^*i \equiv 1 \pmod{p}$. Note that, by our choice of indexing, we have

$$\forall j \in (\mathbb{Z}/\ell\mathbb{Z})^\times, \quad \mathfrak{p}_{z,i} = \mathfrak{p}_{z^j,ij}. \tag{42}$$

What about the splitting type of such a prime ideal $\mathfrak{p}_{z,i}$ in K_c ? Since K_c has prime degree ℓ over $\mathbb{Q}(\zeta_\ell)$ and by (40), each $\mathfrak{p}_{z,i}$ either splits completely or remains inert in K_c . Furthermore, since K_c is Galois over \mathbb{Q} , the splitting type of each $\mathfrak{p}_{z,i}$ is the same. Under the assumptions (40), one has

$$\begin{aligned} \mathfrak{p}_{z,i} \text{ splits completely in } K_c &\iff c \pmod{p} \in (\mathbb{F}_p^\times)^\ell \\ &\iff \theta_c \in \mathbb{F}_p^\times / \mu_\ell \end{aligned} \tag{43}$$

If this is the case, we may allow z in (41) to be an arbitrary generator of $\mu_\ell \subset \mathbb{F}_p^\times$ and note also that, under the isomorphism (39),

$$\mathfrak{p}_{z,i} \text{ splits completely in } K_c \iff \text{Frob}_{\mathfrak{P}} = (1, 0),$$

for any prime ideal $\mathfrak{P} \subseteq \mathcal{O}_{K_c}$ lying over $\mathfrak{p}_{z,i}$.

In case $\mathfrak{p}_{z,i}$ does not split completely in K_c , the finite field $\mathbb{F}_p[\theta_c]$ has degree ℓ over \mathbb{F}_p , and we normalize our choice of $z = z_c \in \mathbb{Z}$ so that

$$\hat{z}_c := \frac{\theta_c^p}{\theta_c} \in \mathbb{F}_p^\times \quad (44)$$

(Note that $\hat{z}_c \in \mathbb{F}_p^\times$ is independent of the choice of $\theta_c \in \overline{\mathbb{F}_p}^\times / \mu_\ell$). In this case, putting

$$\mathfrak{P}_{z_c,i} := \mathfrak{p}_{z_c,i} \mathcal{O}_{K_c} = p \mathcal{O}_{K_c} + (\zeta_\ell - z_c^{i*}) \mathcal{O}_{K_c}, \quad (45)$$

the ideal $\mathfrak{P}_{z_c,i}$ is prime and we have a prime factorization

$$p \mathcal{O}_{K_c} = \prod_{i \in (\mathbb{Z}/\ell\mathbb{Z})^\times} \mathfrak{P}_{z_c,i}.$$

The following lemma characterizes the Frobenius automorphism $\text{Frob}_{\mathfrak{P}_{z_c,i}}$.

Lemma 5.16. *Suppose $c \in \mathbb{Q}^\times$ satisfies $K_c := \mathbb{Q}(\zeta_\ell, c^{1/\ell}) \neq \mathbb{Q}(\zeta_\ell)$. Furthermore, let p be a prime number satisfying $p \equiv 1 \pmod{\ell}$ and $\text{ord}_p(c) = 0$. Then p is unramified in K_c and, with notation as above, under the isomorphism $\text{Gal}(K_c/\mathbb{Q}) \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes \mathbb{Z}/\ell\mathbb{Z}$, one has*

$$\text{Frob}_{\mathfrak{P}_{z_c,i}} = \begin{cases} (1, 0) & \text{if } p \text{ splits completely in } K_c \text{ and } \mathfrak{P}_{z_c,i} \text{ is any prime above } p \\ (1, i) & \text{if } p \mathcal{O}_{K_c} = \prod_{i \in (\mathbb{Z}/\ell\mathbb{Z})^\times} \mathfrak{P}_{z_c,i}, \text{ where each } \mathfrak{P}_{z_c,i} \text{ is as in (45) and is prime.} \end{cases}$$

Proof. We need only concern ourselves with the case that p does not split completely in K_c . In this case, consider the ring homomorphism $\pi_{z_c,i} : \mathcal{O}_{\mathbb{Q}(\zeta_\ell)} \rightarrow \mathbb{F}_p$, induced by $\zeta_\ell \mapsto z_c^{i*} \pmod{p}$. Note that

$$\ker \pi_{z_c,i} = \mathfrak{p}_{z_c,i} \quad \text{and} \quad \sigma_a(\mathfrak{p}_{z_c,i}) = \mathfrak{p}_{z_c,ai},$$

where $\sigma_a \mapsto a$ under $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. Since $\mathcal{O}_{K_c}/\mathfrak{P}_{z_c,i} \simeq \mathbb{F}_p(\theta_c)$ in this case, one may extend $\pi_{z_c,i}$ to a ring homomorphism $\varpi_{z_c,i} : \mathcal{O}_{K_c} \rightarrow \mathbb{F}_p(\theta_c)$ for which $\varpi_{z_c,i}(c^{1/\ell}) = \theta_c$. Consider the induced isomorphism

$$\varpi_{z_c,i} : \mathcal{O}_{K_c}/\mathfrak{P}_{z_c,i} \rightarrow \mathbb{F}_p(\theta_c).$$

By definition of $\text{Frob}_{\mathfrak{P}_{z_c,i}}$, one has $\varpi_{z_c,i} \circ \text{Frob}_{\mathfrak{P}_{z_c,i}} \circ \varpi_{z_c,i}^{-1}(\theta_c) = \theta_c^p$. On the other hand, if $\text{Frob}_{\mathfrak{P}_{z_c,i}} \mapsto (1, b)$ under (39), then by (44), we have

$$z_c \theta_c = \theta_c^p = \varpi_{z_c,i}(\text{Frob}_{\mathfrak{P}_{z_c,i}}(\varpi_{z_c,i}^{-1}(\theta_c))) = \varpi_{z_c,i}(\text{Frob}_{\mathfrak{P}_{z_c,i}}(c^{1/\ell} \pmod{\mathfrak{P}_{z_c,i}})) = \varpi_{z_c,i}(\zeta_\ell^b c^{1/\ell}) = z_c^{i*b} \theta_c.$$

Thus, one finds that $b = i$, proving the lemma. \square

The next corollary of Lemma 5.16 is essential in what follows. We introduce the notation

$$K = \mathbb{Q}(\zeta_\ell, c_1^{1/\ell}, c_2^{1/\ell}, \dots, c_k^{1/\ell}, d_1^{1/\ell}, d_2^{1/\ell}, \dots, d_k^{1/\ell}) =: \mathbb{Q}(\zeta_\ell, \mathbf{c}^{1/\ell}, \mathbf{d}^{1/\ell}),$$

where $\mathbf{c}, \mathbf{d} \in \mathbb{Q}^k$ are the obvious vectors, and

$$\begin{aligned} \text{Gal}(K/\mathbb{Q}) &\hookrightarrow (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes (\mathbb{Z}/\ell\mathbb{Z})^{2k} \\ &= (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes ((\mathbb{Z}/\ell\mathbb{Z})^k \times (\mathbb{Z}/\ell\mathbb{Z})^k), \end{aligned} \quad (46)$$

so that elements of $\text{Gal}(K/\mathbb{Q})$ may be written in the form $(a, \mathbf{b}, \mathbf{f})$ with $\mathbf{b}, \mathbf{f} \in (\mathbb{Z}/\ell\mathbb{Z})^k$. We denote by $\mathcal{C}_{2k} \subseteq \text{Gal}(K/\mathbb{Q})$ the subset

$$\mathcal{C}_{2k} := \{(1, \mathbf{b}, \mathbf{f}) \in \text{Gal}(K/\mathbb{Q}) : \mathbf{f} = \lambda \mathbf{b} \text{ for some } \lambda \in \mathbb{Z}/\ell\mathbb{Z}\}. \quad (47)$$

Note that, under $\text{Gal}(K/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes (\mathbb{Z}/\ell\mathbb{Z})^{2k}$, the subset \mathcal{C}_{2k} is stable by $\text{Gal}(K/\mathbb{Q})$ -conjugation.

Corollary 5.17. *Let $K = \mathbb{Q}(\zeta_\ell, \mathbf{c}^{1/\ell}, \mathbf{d}^{1/\ell})$ and assume the remaining notation just introduced. Let p be any prime number satisfying*

$$\forall i \in \{1, 2, \dots, k\}, \quad \text{ord}_p(c_i) = \text{ord}_p(d_i) = 0$$

and $p \equiv 1 \pmod{\ell}$. Suppose further that, for some fixed $k_p \in \mathbb{Z}/(p-1)\mathbb{Z}$, one has

$$\forall i \in \{1, 2, \dots, k\}, \quad d_i \equiv c_i^{k_p} \pmod{p}.$$

Then p is unramified in K and, under the embedding (46), the Frobenius class $\text{Frob}_p \subseteq \text{Gal}(K/\mathbb{Q})$ satisfies

$$\text{Frob}_p \subseteq \mathcal{C}_{2k}.$$

Proof. Note that, for any vector $\mathbf{w} = (w_1, w_2, \dots, w_m) \in \mathbb{Q}^m$, the diagram

$$\begin{array}{ccc} \text{Gal}(\mathbb{Q}(\zeta_\ell, \mathbf{w}^{1/\ell})/\mathbb{Q}) & \longrightarrow & (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes (\mathbb{Z}/\ell\mathbb{Z})^m \\ \text{res} \downarrow & & \pi_j \downarrow \\ \text{Gal}(\mathbb{Z}(\zeta_\ell, w_j^{1/\ell})/\mathbb{Q}) & \longrightarrow & (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes \mathbb{Z}/\ell\mathbb{Z} \end{array}$$

commutes, where $\pi_j(\mathbf{w}) := w_j$. Taking any prime p as in the statement of the corollary, p is unramified in K , and we fix a prime \mathfrak{P} of K lying over p . By the discussion preceding Lemma 5.16, for any multiplicative generator $z \in \mu_\ell \subseteq \mathbb{F}_p^\times$ we may find $i \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ for which

$$\mathfrak{P} \cap \mathcal{O}_{\mathbb{Q}(\zeta_\ell)} = \mathfrak{p}_{z,i}. \quad (48)$$

Let us fix an index $j \in \{1, 2, \dots, k\}$ and put $c := c_j$ and $d := d_j$. Furthermore, denote by

$$\mathfrak{P}_c := \mathfrak{P} \cap \mathcal{O}_{K_c} \quad \text{and} \quad \mathfrak{P}_d := \mathfrak{P} \cap \mathcal{O}_{K_d}$$

the corresponding primes of $K_c := \mathbb{Q}(\zeta_\ell, c^{1/\ell})$ (resp. of $K_d := \mathbb{Q}(\zeta_\ell, d^{1/\ell})$) lying under \mathfrak{P} . Now if $c \pmod{p} \in (\mathbb{F}_p^\times)^\ell$, then necessarily $d \equiv c^{k_p} \pmod{p} \in (\mathbb{F}_p^\times)^\ell$, and by (43), we have that $\text{Frob}_{\mathfrak{P}_c} = (1, 0) = \text{Frob}_{\mathfrak{P}_d}$ (note that this covers the case $c \in (\mathbb{Q}^\times)^\ell$). In case $k_p \equiv 0 \pmod{\ell}$, we see by the same reasoning that $\text{Frob}_{\mathfrak{P}_d} = (1, 0)$, and one finds that in any of the above cases, the conclusion of the lemma holds, taking $\lambda = 0$ in (47).

We now turn to the case $c \pmod{p} \notin (\mathbb{F}_p^\times)^\ell$ and $\ell \nmid k_p$. In this case, we put $z = z_c$ in (48), possibly adjusting $i \pmod{\ell}$ appropriately. Noting that θ_d only depends on d modulo p , we find that $\theta_d = \theta_c^{k_p}$, and so $z_d = z_c^{k_p}$. Thus, by (45) and (42), we find that

$$\mathfrak{P}_c = \mathfrak{P}_{z_c, i} = \mathfrak{P}_{z_c^{k_p}, i k_p} = \mathfrak{P}_{z_d, i k_p}.$$

Applying Lemma 5.16 and noting that the factor k_p is independent of the index j , we have finished the proof. \square

In particular, taking $\mathbf{c} = (n_1, n_2) \in \mathbb{N}^2$ and $\mathbf{d} = (f(n_1), f(n_2)) \in (\mathbb{Q}^\times)^2$, we obtain the following corollary. Recall that $b_{f, \mathbf{n}} := \left| \prod_{i=1}^2 n_i \text{Num}(f(n_i)) \text{Den}(f(n_i)) \right|$.

Corollary 5.18. *Suppose that $f : \mathbb{Q} \rightarrow \mathbb{Q}$ is any function, $n_1, n_2 \in \mathbb{N}$, and ℓ is an odd prime number which doesn't divide $b_{f, \mathbf{n}}$. Then, with $K = \mathbb{Q}(\zeta_\ell, n_1^{1/\ell}, n_2^{1/\ell}, f(n_1)^{1/\ell}, f(n_2)^{1/\ell})$, one has*

$$p \in S_f \text{ and } p \equiv 1 \pmod{\ell} \implies \text{Frob}_p \subseteq \mathcal{C}_4 \text{ or } p \mid b_{f, \mathbf{n}},$$

where \mathcal{C}_4 is defined by taking $k = 2$ in (47).

5.7. Proof of Proposition 5.3. We now assume that f is not a global power map, and define the constant $a_f > 0$ by

$$a_f := \begin{cases} \min\{\max\{\delta_{f, \mathbf{n}}, e^{b_{f, \mathbf{n}}}\} : \mathbf{n} \in \mathcal{N}_f\} & \text{if } \mathcal{N}_f \neq \emptyset \\ 1 & \text{if } \mathcal{N}_f = \emptyset \end{cases}$$

(since $\delta_{f, \mathbf{n}} \geq 2$, we see that the minimum exists). In case $|S_f| = \infty$, by Corollary 5.12 we have that $\mathcal{N}_f \neq \emptyset$, so we may pick $\mathbf{n} \in \mathcal{N}_f$ for which

$$a_f = \max\{\delta_{f, \mathbf{n}}, e^{b_{f, \mathbf{n}}}\},$$

and then apply Theorem 5.1 with $K = \mathbb{Q}(\zeta_\ell, n_1^{1/\ell}, n_2^{1/\ell}, f(n_1)^{1/\ell}, f(n_2)^{1/\ell})$. Note that in particular, provided $\ell > a_f$, by Corollary 5.18, one has

$$\sum_{\substack{p \in S_f(x) \\ p \equiv 1 \pmod{\ell}}} 1 \leq \pi(x; K/\mathbb{Q}, \mathcal{C}_4) + O(\nu(b_{f, \mathbf{n}})). \quad (49)$$

Our assumption that

$$Z \leq \left(\frac{\log x}{(6c_2 \log \log x)^2} \right)^{1/15} \quad (50)$$

implies that, for x large enough, one has $\sqrt{\log x/Z^5} \geq 6c_2 \cdot Z^5 \log Z$. By Corollary 5.15, $\ell \in [Y, Z)$ and $a_f < Y$ guarantee that (20) holds in this case. Thus, for $Y > a_f$ and $\ell \in [Y, Z)$, one has

$$\begin{aligned} \pi(x; K/\mathbb{Q}, \mathcal{C}_4) &= \frac{|\mathcal{C}_4|}{|\text{Gal}(K/\mathbb{Q})|} \cdot \pi(x) + O\left(|\mathcal{C}_4| \cdot x \cdot \exp\left(-c_1 \sqrt{\frac{\log x}{[K:\mathbb{Q}]}}\right)\right) \\ &\ll \frac{|\mathcal{C}_4|}{|\text{Gal}(K/\mathbb{Q})|} \cdot \pi(x) + \ell^3 \cdot x \cdot \exp\left(-c_1 \sqrt{\frac{\log x}{Z^5}}\right). \end{aligned} \quad (51)$$

The following lemma bounds the first term above.

Lemma 5.19. *Suppose that $f : \mathbb{Q} \rightarrow \mathbb{Q}$ is any function, let $n_1, n_2 \in \mathbb{N}$, let ℓ be an odd prime, and let $K := \mathbb{Q}(\zeta_\ell, n_1^{1/\ell}, n_2^{1/\ell}, f(n_1)^{1/\ell}, f(n_2)^{1/\ell})$. Suppose that*

$$[\mathbb{Q}(\zeta_\ell, n_1^{1/\ell}, n_2^{1/\ell}, f(n_1)^{1/\ell}) : \mathbb{Q}(\zeta_\ell)] = \ell^3. \quad (52)$$

Then one has

$$\frac{|\mathcal{C}_4|}{|\text{Gal}(K/\mathbb{Q})|} \leq \frac{2}{\ell(\ell-1)},$$

where \mathcal{C}_4 is defined by taking $k = 2$ in (47).

Proof. By hypothesis, if ℓ is large enough then either $\text{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes (\mathbb{Z}/\ell\mathbb{Z})^4$ or

$$\text{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes (\mathbb{Z}/\ell\mathbb{Z} \cdot \mathbf{d})^\perp,$$

where $\mathbf{d} = (d_1, d_2, d_3, d_4) \in (\mathbb{Z}/\ell\mathbb{Z})^4$ and

$$d_4 \neq 0, \quad (53)$$

which follows from the hypothesis (52). If $\text{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes (\mathbb{Z}/\ell\mathbb{Z})^4$, then directly from (47) one finds that

$$|\mathcal{C}_4| \leq \ell^3,$$

and the conclusion of the lemma follows. If on the other hand

$$\text{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes (\mathbb{Z}/\ell\mathbb{Z} \cdot \mathbf{d})^\perp,$$

then, writing $\mathbf{d} = (\mathbf{d}_1, \mathbf{d}_2)$ with $\mathbf{d}_i \in (\mathbb{Z}/\ell\mathbb{Z})^2$, we have that

$$\begin{aligned} \mathcal{C}_4 &= \{(1, \mathbf{b}, \lambda \mathbf{b}) : (\mathbf{b}, \lambda) \in (\mathbb{Z}/\ell\mathbb{Z})^3, \mathbf{b} \cdot \mathbf{d}_1 + \lambda \mathbf{b} \cdot \mathbf{d}_2 = 0\} \\ &= \{(1, \mathbf{b}, \lambda \mathbf{b}) : (\mathbf{b}, \lambda) \in (\mathbb{Z}/\ell\mathbb{Z})^3, \mathbf{b} \cdot (\mathbf{d}_1 + \lambda \mathbf{d}_2) = 0\}. \end{aligned}$$

Consider the equation

$$\mathbf{b} \cdot (\mathbf{d}_1 + \lambda \mathbf{d}_2) = 0. \quad (54)$$

By (53) we see that $\mathbf{d}_2 \neq \mathbf{0} \in (\mathbb{Z}/\ell\mathbb{Z})^2$, and so $\mathbf{d}_1 + \lambda \mathbf{d}_2 = \mathbf{0}$ for at most one $\lambda \in \mathbb{Z}/\ell\mathbb{Z}$. For such a λ , one counts ℓ^2 solutions $\mathbf{b} \in (\mathbb{Z}/\ell\mathbb{Z})^2$ to the equation (54), while for each of the other $\ell - 1$ values of λ one counts ℓ solutions. Thus, one has

$$|\mathcal{C}_4| \leq \ell(2\ell - 1),$$

and the conclusion of the lemma follows in this case as well. \square

Inserting the result of Lemma 5.19 into (51) and using (49) we obtain, that, for $\ell \in [Y, Z)$ we have

$$\sum_{\substack{p \in S_f(x) \\ p \equiv 1 \pmod{\ell}}} 1 \ll \frac{1}{\ell^2} \cdot \pi(x) + \ell^3 \cdot x \cdot \exp\left(-c_1 \sqrt{\frac{\log x}{Z^5}}\right) + \nu(b_{f,\mathbf{n}}),$$

provided (50) holds. Summing over primes $\ell \in [Y, Z)$, we obtain

$$\sum_{Y \leq \ell < Z} \sum_{\substack{p \in S_f(x) \\ p \equiv 1 \pmod{\ell}}} 1 \ll \frac{1}{Y \log Y} \cdot \pi(x) + \frac{Z^4}{\log Z} \cdot x \cdot \exp\left(-c_1 \sqrt{\frac{\log x}{Z^5}}\right) + \nu(b_{f,\mathbf{n}}),$$

By virtue of the bounds (50) and (26), we see that the second remainder term satisfies

$$\frac{Z^4}{\log Z} \cdot x \cdot \exp\left(-c_1 \sqrt{\frac{\log x}{Z^5}}\right) \ll_A \frac{x}{(\log x)^A}$$

for any $A > 0$, and since $Y < Z$, this observation finishes the proof of Proposition 5.3.

Remark 5.20. The hypothesis in Lemma 5.19 that f not be a global power map is critical. Indeed, if $f(\alpha) = \alpha^k$ for all $\alpha \in \mathbb{Q}$, then (e.g. provided n_2 is multiplicatively independent from n_1) under (46) one has

$$\text{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes \{(\mathbf{b}, e\mathbf{b}) : \mathbf{b} \in (\mathbb{Z}/\ell\mathbb{Z})^2\}.$$

In particular, one finds that

$$\frac{|\mathcal{C}_4|}{|\text{Gal}(K/\mathbb{Q})|} = \frac{|\{(1, \mathbf{b}, e\mathbf{b}) : \mathbf{b} \in (\mathbb{Z}/\ell\mathbb{Z})^2\}|}{|(\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes \{(\mathbf{b}, e\mathbf{b}) : \mathbf{b} \in (\mathbb{Z}/\ell\mathbb{Z})^2\}|} = \frac{1}{\ell - 1},$$

and our method of proof fails for this case (as it should).

6. ACKNOWLEDGMENTS

This paper was motivated by a question posed by C. Khare in connection with compatible systems of one-dimensional Galois representations. I thank Professor Khare for sharing this interesting question, and also Professor R. Khan, who originally communicated it to me. Some of the research leading to this paper was done during a research stay at the Universität Göttingen, and I would like to thank the university for providing a stimulating environment in which to work. Finally, I would also like to thank Professor S. Basarab for stimulating discussions on this topic and for helpful comments.

REFERENCES

- [1] C. Corrales and R. Schoof. The support problem and its elliptic analogue, *J. Number Theory* **64** (1997), 276–290.
- [2] P. Erdős. On the distribution function of additive functions, *Ann. of Math.* **47** no. 2 (1946), 1–20.
- [3] J. Fabrykowski and M. V. Subbarao. On a class of Arithmetic functions satisfying a congruence property, *J. Madras Univ.*, **51** no. 1 (1988), 48–56.
- [4] J. Fehér and B. M. Phong. On a problem of Fabrykowski and Subbarao concerning quai multiplicative functions satisfying a congruence property, *Acta. Math. Hungar.*, **89** (2000), 149–159.
- [5] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge Studies in Advanced Mathematics **27**, Cambridge Univ. Press (1991).
- [6] R. Gupta and M. R. Murty. A remark on Artin’s conjecture, *Invent. Math.* **78** no. 1 (1984), 127–130.
- [7] D. R. Heath-Brown. Artin’s conjecture for primitive roots, *Quart. J. Math. Oxford* **37** no. 1 (1986), 27–38.
- [8] C. Khare and D. Prasad. Reduction of homomorphisms mod p and algebraicity, *J. Number Theory* **105** (2004), 322–332.
- [9] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem, in A. Frohlich (ed.) *Algebraic Number Fields*, pp. 409–464, Academic Press, 1977.
- [10] S. Lang, *Algebra*, Graduate Texts in Mathematics **211**, Springer (2002).
- [11] I. Ruzsa. On congruence-preserving functions, *Mat. Lap.* **22** (1971), 125–134.
- [12] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Publ. Math. I. H. E. S.* **54** (1981), 123–201.
- [13] M. V. Subbarao. Arithmetic functions satisfying a congruence property, *Canad. Math. Bull.* **9** (1966), 143–146.
- [14] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics **46**, Cambridge Univ. Press (1995).
- [15] L. Washington. *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, **83**. Springer-Verlag, New York, 1982.
- [16] U. Zannier. On periodic mod p sequences and G -functions, *Manuscripta mathematica* **90** no. 3 (1996), 391–402.